(12) UK Patent (19) GB (11) 2 376 392 (13) B

(45) Date of publication: 07.05.2003

(54) Title of the invention: Legal interception of IP traffic

(51) Int Cl[7]: **H04L** 9/08

(21) Application No: **0129339.8**

(22) Date of Filing: **07.12.2001**

(43) Date A Publication: **11.12.2002**

(52) UK CL (Edition V):
H4P PDCSP

(56) Documents Cited:
WO 2001/056222 A1 **WO 1996/005674 A1**

(58) Field of Search:
As for published application 2376392 A *viz:*
UK CL (Edition T) **H4P** PDCSP
INT CL[7] **H04L** 9/08
Other: **Online: WPI, EPODOC, JAPIO, INSPEC**
updated as appropriate

(72) Inventor(s):
Ilkka Mikael Uusitalo
Pasi Matti Kalevi Ahonen

(73) Proprietor(s):
Telefonaktiebolaget LM Ericsson
(Incorporated in Sweden)
S-126 25 Stockholm, Sweden

(74) Agent and/or Address for Service:
Marks & Clerk
4220 Nash Court,
Oxford Business Park South, OXFORD,
OX4 2RU, United Kingdom

2376392

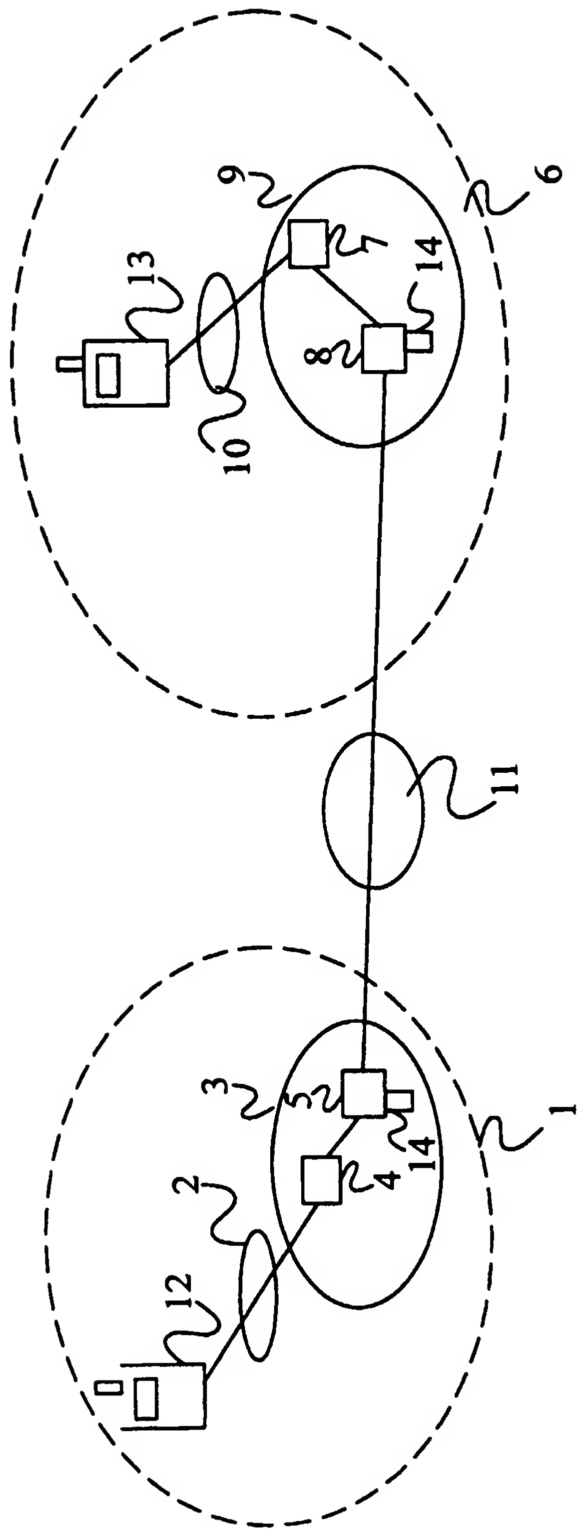

Figure 1

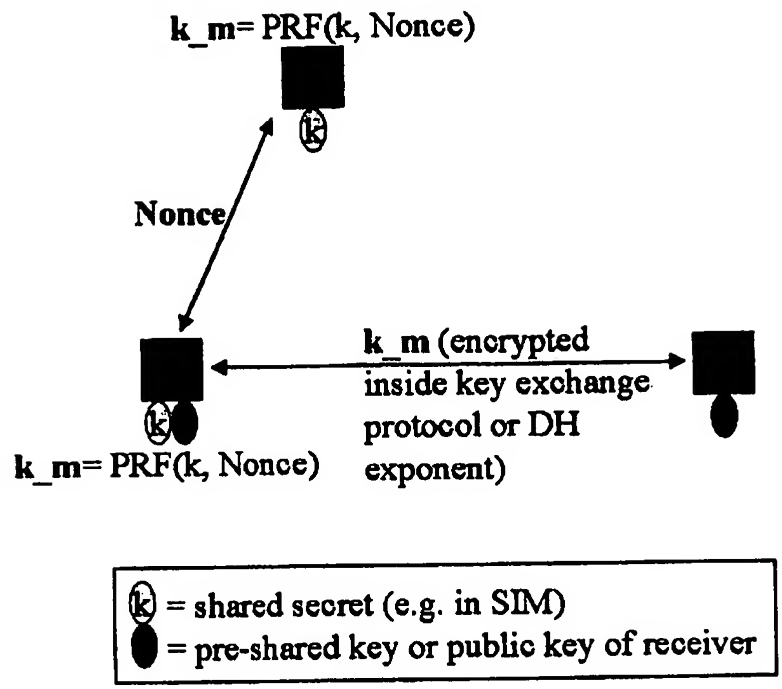
k_m= PRF(k, Nonce)
Nonce
k_m (encrypted inside key exchange protocol or DH exponent)
k_m= PRF(k, Nonce)
k = shared secret (e.g. in SIM)
= pre-shared key or public key of receiver

Figure 2

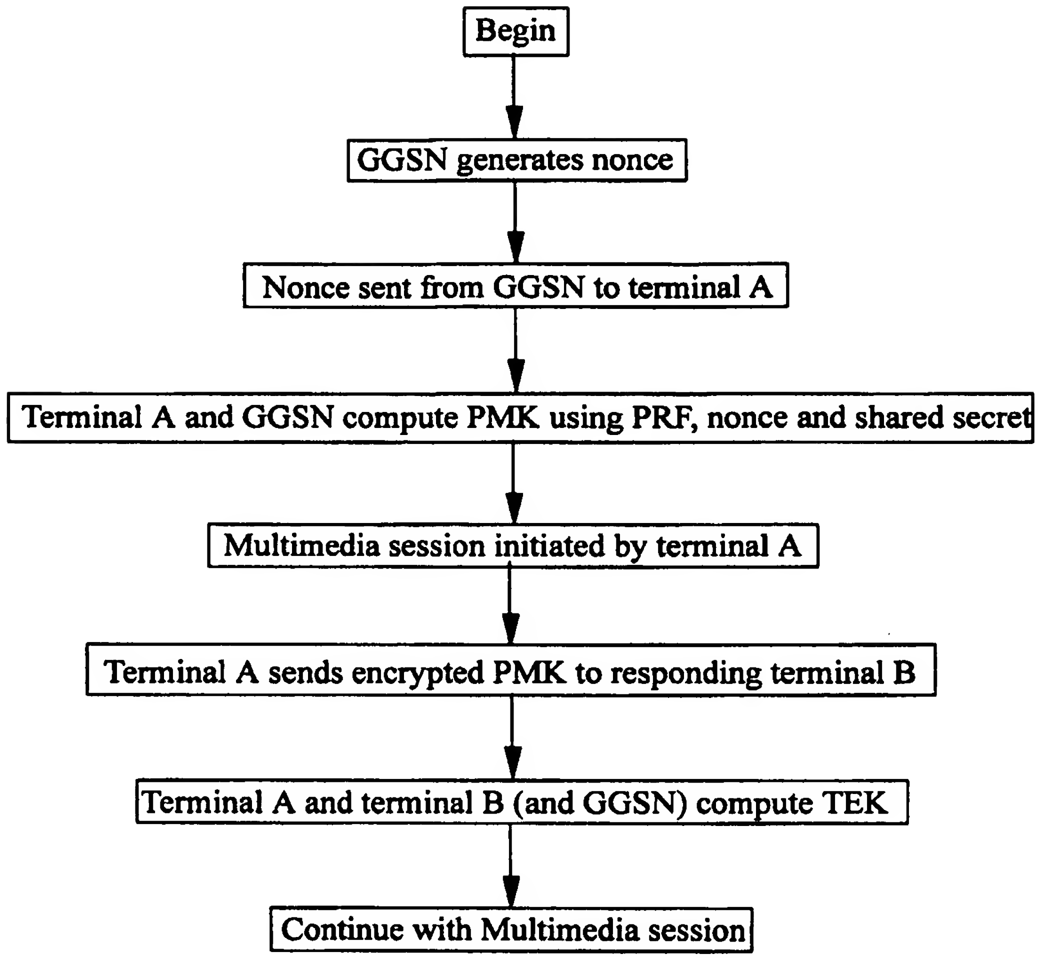
Begin
GGSN generates nonce
Nonce sent from GGSN to terminal A
Terminal A and GGSN compute PMK using PRF, nonce and shared secret
Multimedia session initiated by terminal A
Terminal A sends encrypted PMK to responding terminal B
Terminal A and terminal B (and GGSN) compute TEK
Continue with Multimedia session

Figure 3

Legal Interception of IP traffic

Field of the Invention

The present invention relates to a method and apparatus for facilitating legal interception of IP traffic.

Background to the Invention

It is now possible to establish various forms of connection over the internet including data connections as well as voice and video telephony connections. As the speed and extent of the Internet increases, the use of voice and video telephony can be expected to grow. Whilst current technology tends to restrict IP multimedia sessions to computer terminals coupled to the Internet, tomorrow's technology will provide for IP multimedia sessions between small dedicated telephony terminals, and other mobile devices such as PDAs, palmtop computers etc.

In order to allow such devices to gain widespread acceptance, a key issue which must be addressed is that of security. The two main security concerns are the avoidance of unauthorised eavesdropping, and the need to authenticate terminals involved in a communication (i.e. to ensure that the terminal which a "subscriber" connects to is the terminal which the subscriber intends to connect to and *vice versa*). However, these concerns are not unique to IP multimedia, and are common to many different forms of IP communication. Several protocols exist for securing data traffic using encryption and/or authentication.

One such security protocol is known as IPSec (IETF RFC2401). In order to allow IPSec packets to be properly encapsulated and decapsulated it is necessary to associate security services and a key between the traffic being transmitted and the remote node which is the intended recipient of the traffic. The construct used for this purpose is a "Security Association" (SA). A second security protocol is known as SRTP (Secure Real-Time Protocol) – see draft-ietf-avt-srtp-02.txt (available at

http://search.ietf.org/internet-drafts/draft-ietf-avt-srtp-02.txt). It is expected that the third generation mobile network architecture known as 3GPP will adopt SRTP as the protocol for securing IP traffic. Of course, other protocols such as IPSec may be used in other mobile network architectures.

In the Internet draft "draft-ietf-msec-mikey-00.txt" (available from http://search.ietf.org/internet-drafts/draft-ietf-msec-mikey-00.txt), a key management scheme known as Multimedia Internet KEYing (MIKEY) is described for use in real-time applications. The scheme provides for the creation of a Security Association (SA) and the distribution of a Pre-Master Key (PMK). The PMK is used to derive a Traffic-Encrypting Key (TEK) for each crypto session. More specifically, the TEK is used as the key input to the chosen security protocol, i.e. SRTP for 3GPP.

Summary of the Invention

Traditional circuit switched telephone networks make provision for the legal interception of telephone calls. Such interception must be instigated by the appropriate authorities and is an important weapon against fraud and other crimes. Understandably, it is desirable to make provision for the legal interception of IP sessions (whether pure data, VoIP, video, etc). However, this presents a potential problem as the IP security protocols which will be used have been designed to provide terminal-to-terminal security involving strong encryption.

If the MIKEY proposal is implemented, security mechanisms will rely upon the use of a Pre-Master Key (PMK) which is agreed upon by the parties to an IP session. The PMK may be proposed by the initiator of the session and accepted (or rejected) by the responder, or may be generated using values exchanged between the parties to the session. The agreement of the PMK forms part of an IP Multi-Media key management function. Following the agreement of the PMK, the Multi-Media key management function may encrypt the PMK with a secret which it shares with the responder, or with the public key of the responder, or the initiator may calculate a Diffie-Hellman modular exponentiation using the PMK as an exponent. It will be appreciated that in order to

intercept traffic associated with that session, a third party must have knowledge of the PMK.

It is an object of the present invention to facilitate the legal interception of an IP session which requires the parties involved in the session to agree upon a PMK for use in securing traffic sent over the session.

According to a first aspect of the present invention there is provided a method of facilitating the legal interception of an IP session between two or more terminals, wherein said session uses encryption to secure traffic, the method comprising:

storing a key allocated to at least one of said terminals or to at least one of the subscribers using one of the terminals, at the terminal and at a node within a network through which said session is conducted;

prior to the communication of a session setup request from the calling terminal to the called terminal, exchanging a seed value between the terminal at which the key is stored and said node, and applying a security function to the key and the seed value at both the terminal and the node to generate a pre-master key, wherein the pre-master key subsequently also becomes known to the or each terminal involved in the IP session; and

directly or indirectly using said pre-master key to encrypt and decrypt traffic associated with said session.

The steps of exchanging the seed value between the terminal and the network node, and of generating a pre-master key are preferably carried out each time a new session is to be created. More preferably, these steps are carried out for every IP session regardless of whether or not legal interception is required.

Preferably, the terminal which exchanges the seed value with the network node and at which a pre-master key is generated is the terminal which initiates the IP session.

The security function which is applied to the seed value and the shared key is preferably a pseudo-random function. Alternatively, the security function may be an encryption function. For some security protocols, the security function may be applied to the seed

value and the shared key in combination with a further seed value identified to the terminal by the other or another terminal involved in the session.

Preferably, the pre-master key is used by the terminals involved in the IP session, and optionally said network node, to generate one or more traffic encryption keys. The traffic encryption key(s) is(are) used to encrypt the traffic associated with the IP session.

Preferably, said network is a mobile telecommunications network, and said terminal with which the node exchanges a seed value is a mobile wireless terminal. The network is typically the home network of that terminal, although this need not be the case.

Preferably, the seed value is a randomly generated value, i.e. a nonce. Alternatively, the seed value may be a parameter associated with the cryptographic session (e.g. a crypto session ID) or with some other function/operation.

According to a second aspect of the present invention there is provided a method of intercepting an IP session set up using the method of the above first aspect, the method comprising intercepting IP data associated with said session at said network node or at another node coupled to that network node, and directly or indirectly using the pre-master key to decrypt the encrypted traffic.

In one embodiment of the second aspect of the invention, the pre-master key or a traffic encryption key (or keys) is sent to an external node and the encrypted traffic is forwarded to that node from the network node for decryption. In an alternative embodiment, IP traffic is intercepted at said network node and is forwarded to a node outside of the network following decryption.

According to a third aspect of the present invention there is provided a terminal for conducting an encrypted IP session with one or more other terminals, the terminal comprising:

a memory for storing a key allocated to the terminal or to a subscriber using the terminal;

means for exchanging a seed value between the terminal and a node of a communications network over which said encrypted IP session is to be conducted, prior to the communication of a session setup request between the communicating terminals;

means for applying a security function to the key and the seed value at the terminal to generate a pre-master key which pre-master key subsequently becomes known to each of the terminals involved in the IP session; and

means for directly or indirectly using pre-master key to encrypt and decrypt traffic associated with said session.

According to a fourth aspect of the present invention there is provided a network node for use in intercepting encrypted traffic associated with an IP session conducted between two or more terminals coupled to a communications network, the node comprising:

a memory storing keys allocated to terminals or subscribers registered with the network;

means for exchanging seed values with terminals prior to the communication of of a session setup request between terminals and the establishment of IP sessions involving the terminals;

means for applying a security function to the key and the seed value to generate a pre-master key; and

means for directly or indirectly using said pre-master key to decrypt traffic associated with said session which is intercepted by the node.

Brief Description of the Drawings

Figure 1 illustrates schematically a communications network for enabling an IP session to be established between two mobile terminals;

Figure 2 shows signalling exchanged between the mobile terminals of Figure 1 and a network node, the signalling being associated with the establishment of a shared secret; and

Figure 3 is a flow diagram illustrating a method of intercepting an IP session.

Detailed Description of a Preferred Embodiment

There is illustrated in Figure 1 a communications system comprising a mobile telecommunications network 1 which for the purpose of this discussion is assumed to be a 3GPP (or UMTS) network. Within the 3GPP network 1 are a UMTS Terrestrial Radio Access Network (UTRAN) 2 and a GPRS network 3. The GPRS network comprises one or more Serving GPRS Support nodes (SGSNs) 4 and one or more Gateway GPRS Support Nodes (GGSNs) 5. The role of the SGSN 4 is to maintain subscription data (identities and addresses) and to track the location of user equipment (UE) within the network. The role of the GGSN 5 is to maintain subscription information and allocated IP addresses and to track the SGSN 4 to which UEs are attached.

Figure 2 also illustrates a second mobile telecommunications network 6 which is also assumed to be a 3GPP network. This network also comprises SGSNs 7 and GGSNs 8 forming part of a GPRS network 9, and a UTRAN 10. The two GGSNs 5,8 are both coupled to an IP network 11. Two UEs 12,13 are attached to the first and second networks 1,6 respectively. 3GPP provides UEs with an "always connected" service such that as long as UEs are registered with a network (home or visited) they are allocated IP addresses and can receive and send data without the need for a connection to be established. A protocol such as Session Initiation Protocol (SIP) may be used to establish a multimedia session between the two UEs 12,13 of Figure 1. Within the GPRS networks 3,9 it is the GGSNs 5,8 which implement the policy of the network operator, e.g. which subscribers can access which services, subscriber priorities, etc.

Typically, when a subscriber registers with the operator of a 3GPP network, he or she receives a Subscriber Identity Module (SIM) card on which is stored a unique International Mobile Subscriber Identity (IMSI) code. In addition to the IMSI it is proposed here that a secret key *k* is also stored on the SIM card. This key is known only to the network operator and to the user (or rather to the user's SIM card) and a copy of the key is stored in a database 14 attached to the GGSN 5,8 of the subscriber's home network. Also stored on the subscriber's SIM card (or possibly in a memory of the subscriber's UE) and in the GGSN 5,8 is a pseudo-random function such as a keyed hash (or MAC, Message Authentication Code) such as SHA-1 or MD5.

For the reasons set out above, it may be necessary to intercept an IP session between the two UEs 12,13. Interception is carried out as follows.

Assume that an IP multimedia session is initiated by a first of the UEs 12. The UE 12 sends a SIP Invite message to the GGSN 5 to which it is attached. The SIP Invite message identifies both the initiating UE 12 and the responding UE – in this case UE 13. At this stage, the GGSN 5 places the session initiation on hold, and inspects the local database 14 to see if it holds a key for the initiating UE 12. If no key is contained in the database 14, the session initiation is not allowed to continue and a notification message may be returned to the UE 12. If on the other hand a key is held for the UE 12, the GGSN 5 generates a random number or "nonce" and returns this to the UE 12. The nonce need not be secured (i.e. encrypted) for transmission to the UE 12. Both the UE 12 and the GGSN 5 then compute a Pre-Master Key (PMK), k_m, by applying the pseudo-random function to the shared key and the nonce, i.e.

$$k\_m = PRF(k, nonce).$$

Once the PMK has been established, the GGSN 5 routes the SIP message to the home network 6 of the responding UE 13 via an IP Multimedia Core Network Subsystem (not shown in Figure 1). The SIP Invite message is received by the responding UE 12 via the GGSN 8 to which it is connected. Assuming that the responding UE 13 chooses to accept the session setup request, phase 1 of the SRTP is initiated. This requires that the UE 12 send to the UE 13 the PMK which has been established by the UE 12 in conjunction with the GGSN 5. The PMK may be encrypted with a secret shared between the UEs 12,13 or with the public key of the responding UE 13 (SRTP does not specify how the PMK should be exchanged or negotiated, it only requires that a common, secret PMK must be known to the parties). In either case, the result is that the UEs 12,13 and the GGSN 5 to which the originating UE 12 is attached, all know the PMK at the end of phase 1.

In phase 2 of the SRTP, the UEs 12,13 use the shared PMK to generate a Traffic-Encrypting Key (TEK). The procedure involved is set out in the MIKEY draft referred

to above. As the algorithm and parameters (including the PMK) required to calculate the TEK are known to the GGSN 5, the GGSN can compute the TEK. Once the TEK is generated, the IP session can begin. Traffic is encrypted and decrypted at the UEs 12,13 using the TEK. In some cases, a pair of TEKs may be generated in phase 2 of the SRTP, with a first of the TEKs being used to encrypt traffic in one direction and the second TEK being used to encrypt traffic in the opposite direction.

It will be appreciated that IP traffic associated with the session will always pass through the GGSN 5. As such, the GGSN 5 is able to intercept the traffic and decrypt it using the TEK(s). The decrypted traffic can then be passed to a government authority such as the police. Alternatively, during the session setup phase, the network operator may forward the TEK(s) to the government authority. Traffic which is intercepted at the GGSN 5 is therefore passed directly to the government authority which can decrypt the traffic using the previously received TEK(s).

The signalling associated with the PMK generation and exchange phase is illustrated in Figure 2. Figure 3 is a flow diagram further illustrating the mechanism. It will be appreciated that the GGSN will only compute the TEK if legal interception is authorised for the IP session.

Agreements may be made between governments and network operators to enable a government authority to intercept an IP session initiated by a UE outside the authority of an interested government. In this case, a PMK generated at a node of an external network may be sent from the external network to the network under the authority of the interested government. The PMK can then be used to intercept the IP session.

Whilst the above description has been concerned with UEs and mobile networks, the present invention is not to be considered limited to mobile networks. The invention is also applicable to IP sessions extending between terminals coupled to fixed line networks and to other wireless networks, and to IP sessions extending between terminals coupled to different network types (e.g. a mobile to fixed line terminal

session). The invention may be applied to UEs connected to the same access network as well as to different access networks.

It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiment without departing from the scope of the present invention. For example, rather than the initiating UE generating the PMK, the PMK may be generated using a Diffie-Hellman exchange between the participating UEs. This involves the sending of a nonce from the GGSN to the initiating UE. Both the UE and the GGSN apply the pseudo-random function to the nonce and the shared secret to generate a value x. The UE generates an exponentiation of a value g to the power x, according to $g^{**}x$, where g is a non-secret value known to the participating UEs and to the GGSN. The computed value is sent to the responding UE. The responding UE then generates a random value y and computes $g^{**}y$, and returns this to the initiating UE. Both parties now calculate a PMK according to $k\_m = g^{**}(xy)$. During this process, the GGSN 3 can intercept the value $g^{**}y$ sent from the responding UE to the initiating UE. As the GGSN already knows the value of x, it can compute the PMK.

In another modification, rather than using a pseudo-random function to generate the PMK from the nonce and the shared secret, an encryption function such as DES or AES may be used. In another modification, rather than using the entire shared secret k to generate the PMK, only a portion or modified version of the shared secret may be used. In yet another modification, the TEK(s) is (are) derived from the PMK via one or more intermediate encryption keys.

Claims

1. A method of facilitating the legal interception of an IP session between two or more terminals, wherein said session uses encryption to secure traffic, the method comprising:

storing a key allocated to at least one of said terminals or to at least one of the subscribers using one of the terminals, at the terminal and at a node within a network through which said session is conducted;

prior to the communication of a session setup request from the calling terminal to the called terminal, exchanging a seed value between the terminal at which the key is stored and said node, and applying a security function to the key and the seed value at both the terminal and the node to generate a pre-master key, wherein the pre-master key subsequently also becomes known to the or each other terminal involved in the IP session; and

directly or indirectly using said pre-master key to encrypt and decrypt traffic associated with said session.

2. A method according to claim 1, wherein the steps of exchanging the seed value between the terminal and the network node, and of generating a pre-master key are carried out each time a new IP session is to be established.

3. A method according to claim 2, wherein the steps of exchanging the seed value between the terminal and the network node, and of generating a pre-master key are carried out for every IP session regardless of whether or not legal interception is required.

4. A method according to any one of the preceding claims, wherein the terminal which exchanges the seed value with the network node and at which a pre-master key is generated is the terminal which initiates the IP session.

5. A method according to any one of the preceding claims, wherein said security function which is applied to the seed value and the shared key is a pseudo-random function.

6. A method according to any one of the preceding claims, wherein the security function is applied to the seed value and the shared key in combination with a further seed value identified to the terminal by the other or another terminal involved in the IP session.

7. A method according to any one of the preceding claims, wherein the pre-master key is used by the terminals involved in the IP session and said network node to generate one or more traffic encryption keys, the traffic encryption key(s) being used to encrypt the traffic associated with the IP session.

8. A method of intercepting an IP session set up using the method of any one of the preceding claims, the method comprising intercepting IP data associated with said session at said network node or at another node coupled to that network node, and directly or indirectly using the pre-master key to decrypt the encrypted traffic.

9. A method according to claim 8, wherein IP traffic is intercepted at said network node and is forwarded to a node outside of the network following decryption.

10. A method according to claim 8, wherein the pre-master key or a traffic encryption key or keys is or are sent to an external node and the encrypted traffic is forwarded to that node from the network node for decryption.

11. A terminal for conducting an encrypted IP session with one or more other terminals, the terminal comprising:

a memory for storing a key allocated to the terminal or to a subscriber using the terminal;

means for exchanging a seed value between the terminal and a node of a communications network over which said encrypted IP session is to be conducted, prior to the communication of a session setup request between the communicating terminals;

means for applying a security function to the key and the seed value at the terminal to generate a pre-master key which pre-master key subsequently becomes known to each of the terminals involved in the IP session; and

means for directly or indirectly using pre-master key to encrypt and decrypt traffic associated with said session.

12. A network node for use in intercepting encrypted traffic associated with an IP session conducted between two or more terminals coupled to a communications network, the node comprising:

a memory storing keys allocated to terminals or subscribers registered with the network;

means for exchanging seed values with terminals prior to the communication of of a session setup request between terminals and the establishment of IP sessions involving the terminals;

means for applying a security function to the key and the seed value to generate a pre-master key; and

means for directly or indirectly using said pre-master key to decrypt traffic associated with said session which is intercepted by the node.